

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA**

<b>AMERICAN CIVIL LIBERTIES UNION, <i>et al.</i></b>	)	
	)	
<b>Plaintiffs,</b>	)	
	)	
v.	)	<b>Civil Action No. 02-2077 (ESH)</b>
	)	
<b>U.S. DEPARTMENT OF JUSTICE</b>	)	
	)	
<b>Defendant.</b>	)	
	)	

**MEMORANDUM OPINION**

In response to the events of September 11, 2001, Congress enacted the USA PATRIOT Act,<sup>1/</sup> which gave federal officials greater power to conduct surveillance within the United States for purposes of both preventing terrorism and monitoring the activity of foreign intelligence agents. In this case, plaintiffs have brought an action under the Freedom of Information Act, 5 U.S.C. § 552 (“FOIA”), seeking information about how the Department of Justice (“DOJ”) has used this new authority. As helpfully narrowed by the parties, the instant dispute centers on certain records that DOJ claims are protected from disclosure by two FOIA exemptions.

Specifically, the information at issue concerns the number of times DOJ has used the particular surveillance and investigatory tools authorized by the Patriot Act since the statute took effect.

To protect this information from disclosure, defendant first invokes Exemption 1, which authorizes the withholding of records “specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and . . . in

---

<sup>1/</sup> “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001,” Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001) (“The Patriot Act”).

fact properly classified pursuant to such Executive order.” 5 U.S.C. § 552(b)(1). Defendant further relies upon Exemption 5, which shields “inter-agency or intra-agency memorandums or letters which would not be available by law to a party . . . in litigation with the agency.” *Id.* at § 552(b)(5). In response to these withholdings, plaintiffs argue that Exemption 1 does not preclude disclosure because the aggregate statistical data at issue here should not have been classified, and that Exemption 5 is inapplicable because they seek only factual information that can readily be segregated from those records properly protected by the deliberative process privilege.

Both parties have now moved for summary judgment on these issues. For the reasons given below, the Court concludes that DOJ’s assertion of Exemption 1 is appropriate, and that the dispute about Exemption 5 is largely illusory. Indeed, it is clear from the Court’s *in camera* review of the Exemption 5 material that, with only one exception, the documents at issue are not responsive to plaintiffs’ request because they do not contain the statistical information the withholding of which plaintiffs now contest. And, insofar as one document does contain statistics of the sort that plaintiffs seek, that information has in fact been properly withheld under Exemption 1. Accordingly, the Court will grant defendant’s motions for summary judgment, and deny plaintiffs’ motion.

## **BACKGROUND**

President Bush signed the Patriot Act into law on October 26, 2001. Of direct relevance to the present action, the statute includes several provisions designed to give law enforcement officers greater authority to conduct certain kinds of surveillance and searches. Most of these changes take the form of amendments to the Foreign Intelligence Surveillance Act of 1978, 50

U.S.C. § 1801 et seq. (“FISA”).<sup>2/</sup> First, section 214 of the Patriot Act drops FISA’s restriction on the use of pen registers and trap and trace devices<sup>3/</sup> against U.S. citizens and lawful permanent aliens (whom FISA calls “U.S. persons,” 50 U.S.C. § 1801(i)). Under the amendment, these tools may now be used against such persons, provided that the information sought is certified as being “relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the

---

<sup>2/</sup> As originally enacted, FISA allowed specially designated judges to authorize electronic surveillance “to obtain foreign intelligence information” if there is “probable cause to believe that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power” and “each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power.” 50 U.S.C. § 1805(a)(3); *see generally In re Sealed Case*, 310 F.3d 717, 722-28 (Foreign Int. Surv. Ct. Rev. 2002). The statute was amended in 1994 to authorize physical searches (according to more or less the same standards), Pub. L. No. 103-359, 108 Stat. 3444 (Oct. 14, 1994), and again in 1998 to permit the use of pen registers and to allow the FBI to obtain access to certain business records in the context of antiterrorism and counterintelligence investigations, Pub. L. No. 105-272, 112 Stat. 2396, §§ 601-02 (Jan. 27, 1998).

<sup>3/</sup> “A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed.” *United States v. New York Tel. Co.*, 434 U.S. 159, 161 n.1 (1977). Pen registers are generally used to record the telephone number dialed by the subject of the surveillance. “Trap and trace” devices, in contrast, are used to record the telephone numbers of incoming calls received by the subject. *See U.S. Telecom Ass’n v. FBI*, 276 F.3d 620, 623 (D.C. Cir. 2001).

Another section of the Patriot Act expands the definition of pen registers and trap and trace devices so that they may be used not merely against telephones, but also against electronic communications (such as e-mail). Under these augmented definitions, pen registers allow officers to determine the routing and addressing information of a surveillance subject’s outgoing e-mail (but not the actual contents of the communication), while a tap and trace device permits similar information to be gathered from the incoming messages that the subject receives. *See Patriot Act*, § 216, *codified at* 18 U.S.C. § 3127(3)-(4).

Constitution.” Patriot Act, § 214, *codified at* 50 U.S.C. § 1842(a)(1); (c)(2).<sup>4/</sup> Before section 214 was enacted, FISA did not allow the use of pen registers and tap and trace devices against U.S. persons. Such authority could, however, be obtained outside of FISA, upon the certification of a federal or state law enforcement officer that the information “likely to be obtained is relevant to ongoing *criminal* investigation.” 18 U.S.C. § 3122(b)(2) (emphasis added).

Next, section 215 amends section 502 of FISA to authorize the FBI to “make an application for an order requiring the production of any tangible things (including books, records, papers, documents, or other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.” Patriot Act, § 215, *codified at* 50 U.S.C. § 1861(a)(1). This amendment substantially expanded the old provision in FISA, under which the FBI could compel only the disclosure of certain business records (rather than “any tangible things”) in the possession of a limited subset of entities: a “common carrier, public accommodation facility, physical storage facility, or vehicle rental facility.” Pub. L. No. 105-272, § 602 (Oct. 20, 1998). What’s more, the Patriot Act eliminated another significant limitation on the use of this authority: the requirement that there be “specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power.” *Id.* Now, in order to gain access to information

---

<sup>4/</sup> Section 214 also dropped FISA’s requirement that applications for pen registers and trap and trace devices include a certification that the communication device in question had been used, or was about to be used, in order to contact a person involved in international terrorism, clandestine intelligence activities, or the agent of a foreign power. Patriot Act, § 214(a)(3), repealing 50 U.S.C. § 1842(c)(3). This change had the effect of lowering the standard for all pen register/tap and trace applications under FISA, not merely those sought for U.S. persons.

covered by section 215, the FBI need only specify that the “records concerned are sought for an authorized investigation . . . to protect against international terrorism or clandestine intelligence activities.” 50 U.S.C. § 1861(b)(2).

A third change to FISA concerns the use of so-called “roving” surveillance. With a roving wiretap, the government can intercept all of a suspect’s communications relating to the conduct under investigation, regardless of the suspect’s location, and regardless of what particular phone or e-mail account he may be using. This usually requires enlisting third parties other than those mentioned in the original surveillance order to install the monitoring device. Thus, under section 206 of the Patriot Act, a court approving a FISA order may direct common carriers, landlords, custodians, or other specified persons to furnish assistance necessary to accomplish the authorized electronic surveillance “in circumstances where the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specific person.” Patriot Act, § 206, *codified at* 50 U.S.C. § 1805(c)(2)(B). With this provision in place, the government need not return to court for a new surveillance order every time the target changes location, but instead can present a generic order to the new carrier, landlord, or custodian, “directing their assistance to assure that the surveillance may be undertaken as soon as technically feasible.” H.R. REP. NO. 107-236(I), at 60 (Oct. 11, 2001).

Finally, the Patriot Act expanded the government’s information-gathering powers in at least one other way unrelated to FISA. Section 213 provides explicit authority for federal law enforcement officers to use so-called “sneak-and-peek” warrants. Such warrants allow agents to conduct searches secretly (whether physically or virtually), to observe or copy evidence, and to depart the location searched, generally without taking any tangible evidence or leaving notice of their presence. *See* Congressional Research Service, *The USA Patriot Act: A Legal Analysis* at

62-63 (Apr. 15, 2002). Before the enactment of the Patriot Act, a court's ability to approve a sneak-and-peek warrant under FED. R. CRIM. P. 41, which clearly required notice when tangible property is actually seized, was not entirely settled. *E.g., United States v. Pangburn*, 983 F.2d 449, 453-55 (2d Cir. 1993) (holding that Rule 41 also requires that notice be provided where a search warrant "authorizes covert entry to seize intangibles"). Section 213 clarified the issue, specifically allowing officers to delay giving notice to the subject of a search if the court issuing the warrant "finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result." Patriot Act, § 213, *codified at* 18 U.S.C. § 3103a(b). Moreover, although in more limited circumstances, these new warrants may also authorize the seizure of tangible property.<sup>5/</sup>

Ever since it was proposed, the Patriot Act has engendered controversy and debate. The Justice Department, which is largely responsible for its implementation, has provided only limited information to the public regarding how, and how often, the new provisions described above have been used.<sup>6/</sup> In June 2002, the House Judiciary Committee asked DOJ to respond in

---

<sup>5/</sup> Specifically, the warrant must prohibit the seizure of tangible property and most wire and electronic information, unless the court finds "reasonable necessity for the seizure." Patriot Act, § 213, *codified at* 18 U.S.C. § 3103a(b)(2). This clause allows for the modification of the requirement in Rule 41(f) (and perhaps in the Constitution as well) that notice be provided at the time that property is actually taken. *Cf. City of West Covina v. Perkins*, 525 U.S. 234, 240 (1999) (suggesting that "when law enforcement agents seize property pursuant to warrant, due process requires them to take reasonable steps to give notice that the property has been taken so the owner can pursue available remedies for its return"). However, section 213 does mandate that the sneak-and-peek warrant set a time for the provision of notice "within a reasonable period of its execution," which period the issuing court can extend for good cause. 18 U.S.C. § 3103a(b)(3).

<sup>6/</sup> On April 29, 2003, the Attorney General reported that 1,228 applications were made to the FISA Court for either electronic surveillance or physical searches during calendar year 2002. All of these applications were ultimately approved. *See Report from John Ashcroft, Attorney General, to L. Ralph Mechem, Director, Administrative Office of the United States Courts*

writing to a series of 50 questions concerning the Department's implementation of the statute. While DOJ provided answers to these questions in two letters dated July 29 and August 26, it deemed some of its answers to be classified, and thus provided them at first only to the House Permanent Select Committee on Intelligence ("HPSCI"). (Letter from Daniel Bryant, Assistant Attorney General to Congressman James Sensenbrenner, Jr., July 26, 2002.) Specifically, the answers to six of these questions "required the disclosure of sensitive FISA operational intelligence information," and therefore were classified at the SECRET level.<sup>7/</sup> (Def.'s Mot. for Summ. J., ex. 4 [Letter from Daniel Bryant, Assistant Attorney General to Congressman Richard A. Gephardt, Oct. 22, 2002].) While Chairman James Sensenbrenner of the House Judiciary Committee ultimately received some of these classified answers, they were not (and have not been) made available to the public. (Mem. in Support of Pls.' Mot. for Summ. J. at 4 & n.5.)

---

(Apr. 29, 2003). This disclosure was made pursuant to 50 U.S.C. § 1807, which requires that such a report be provided in April of each year.

<sup>7/</sup> The questions to which the classified answers were provided concerned the number of times that DOJ had used its new powers to obtain roving surveillance orders (questions 8 and 27), pen registers/trap and trace devices against U.S. persons (question 10), and tangible objects/business records in the context of terrorism investigations (questions 11-12). A final question (question 15) asked how many U.S. persons had been subject to new FISA surveillance orders since the enactment of the Patriot Act. (Letter from House Judiciary Committee to John Ashcroft, Attorney General, June 13, 2002.)

Interestingly, FISA itself requires that the Attorney General provide similar information to the Committee on a semiannual basis. Section 306 of FISA entitles the House and Senate Judiciary Committees to receive a report every six months setting forth the number of physical searches approved under FISA, the number denied, and the number that involved searches of U.S. persons. *See* 50 U.S.C. § 1826. Section 406 requires the Attorney General to provide a similar accounting of the total number of orders approving and denying the use of pen registers/trap and trace devices. *See* 50 U.S.C. § 1846(b). And section 502 of the statute mandates the same semiannual report with respect to the number of orders approved and denied for the production of tangible things under FISA. *See* 50 U.S.C. § 1862(b). These provisions also set forth more detailed disclosure requirements that the Attorney General must meet in order to keep HPSCI, as well as the corresponding Senate Select Committee on Intelligence, fully informed regarding DOJ's use of its FISA tools.

Plaintiffs' FOIA request, which was filed in August 2002, represents an attempt to compel the Department to be more forthcoming. Three basic categories of information were sought. First, plaintiffs requested all records prepared or collected by DOJ in connection with the classified answers, some of which they believe were improperly classified. Second, they asked for policy directives and other guidance materials issued by DOJ regarding the use of certain surveillance techniques authorized by the Patriot Act. Third, and most importantly for this case, plaintiffs sought records containing aggregate statistical information revealing how often DOJ had used the Act's new surveillance and search provisions: roving surveillance under section 206; pen registers/trap and trace devices under section 214; demands for production of tangible things under section 215; and sneak and peek warrants under section 213. (Mem. in Support of Pls.' Mot. for Pre. Inj. at 12-15.)

Plaintiffs also requested expedited processing of their FOIA request, which defendant granted on September 3, 2002. On October 16, however, defendant indicated that it had not yet completed its search for responsive records, which led plaintiffs to file this action on October 24. They then filed a motion for a preliminary injunction on November 13, seeking to force DOJ to respond to their request immediately. After this Court held a hearing on November 26, both sides agreed that defendant would complete its processing by January 15, 2003. After DOJ sought and received several extensions of this deadline, it finished work on plaintiffs' request on March 3. Three separate components of DOJ handled this request: the Office of Information and Privacy ("OIP"); the Office of Intelligence Policy and Review ("OIPR"); and the FBI.

OIP searched for and reviewed records located in the Department's senior leadership offices. Ultimately, it identified 166 pages of responsive, nonpublic documents, and released 108 of these pages in their entirety. OIP released an additional 52 pages with excisions either

pursuant to FOIA Exemptions 5, 6, and 7(C), or of material not responsive to plaintiffs' request.<sup>8/</sup> The remaining six pages were referred to OIPR for processing. (Second Decl. of Melanie Pustay [Sec. Pustay Decl.] ¶¶ 9, 11.) In turn, OIPR, the component directly responsible for preparing applications for electronic surveillance and physical searches under FISA, located 34 responsive documents (68 pages), mostly e-mail messages discussing the Department's responses to the House Judiciary Committee's questions. (Decl. of James A. Baker [Baker Decl.] ¶ 8.) Two of these documents were released unredacted. Twenty-two additional documents were released with excisions, pursuant to Exemptions 5 and 6. Eight remaining documents were withheld in their entirety, based on Exemptions 1, 5, and 6. The two final documents were referred to OIP and the FBI for their review and direct response. (*Id.* at ¶ 11.) Finally, the FBI released a total of 157 pages of documents, some of which were redacted. In addition, 50 full pages were withheld based on Exemptions 1, 2, 5, 7(C), and 7(E).<sup>9/</sup> (Revised Second Decl. of Christine Kiefer [Kiefer Decl.] ¶¶ 10-11.)

As noted, plaintiffs have now waived all challenges to withholdings under Exemptions 2,

---

<sup>8/</sup> Exemption 6 prevents the disclosure of files which "would constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(6). Similarly, Exemption 7(C) protects records compiled for law enforcement purposes, the production of which "could reasonably be expected to constitute an unwarranted invasion of personal privacy." *Id.* at § 552(b)(7)(C). Plaintiffs have indicated that they do not challenge defendant's withholdings pursuant to these exemptions. (Mem. in Supp. of Pls.' Mot. for Summ. J. at 8 & n.8.)

<sup>9/</sup> Exemption 2 exempts information "solely related to the internal personnel rules and practices of an agency," while 7(E) protects law enforcement records that "would disclose techniques and procedures for law enforcement investigations and prosecutions." 5 U.S.C. §§ 552(b)(2), (7)(E). Plaintiffs do not challenge the FBI's withholdings, except insofar as the Bureau relies on Exemption 1 to withhold 14 pages of documents, and Exemption 5 to withhold an additional 50 pages (and portions of 10 more), but only insofar as these documents contain statistical information regarding the Bureau's overall use of particular surveillance tools. (Mem. in Supp. of Pls.' Mot. for Summ. J. at 9-10 & n.10.)

6, and 7. In addition, plaintiffs have dropped their challenge to the adequacy of defendant's searches. (Mem. in Supp. of Pls.' Mot. for Summ. J. at 8-10 & nn.8-10.) As such, the only remaining issue in this case is whether OIP, OIPR, and the FBI properly invoked Exemptions 1 and 5 to justify the withholding of aggregate, statistical data concerning the extent to which DOJ has used its new powers under the Patriot Act to conduct particular forms of surveillance and searches. The universe of such documents is not vast. Under Exemption 1, the contested withholdings involve two full documents located by OIPR and portions of 14 documents located by the FBI. Under Exemption 5, plaintiffs object to the withholding of portions of 26 documents identified by OIP, six complete documents and portions of 18 more by OIPR, and 50 full pages, along with portions of 10 additional pages, by the FBI. It is to the merits of these challenges that the Court now turns.

## ANALYSIS

### I. FOIA: General Principles and Standard of Review

FOIA was enacted in 1966 to implement a "general philosophy of full agency disclosure unless information is exempted under clearly delineated statutory language." *Dep't of the Air Force v. Rose*, 425 U.S. 352, 360-61 (1976) (quoting S. Rep. No. 89-813 (1965)). Thus, an agency must promptly make available any records requested by members of the public, unless the agency can establish that the information is properly withheld under any of the nine exemptions set forth in the statute. *See* 5 U.S.C. § 552(b). These exemptions are exclusive, and should be narrowly construed. *Rose*, 425 U.S. at 361. When a challenge is made to an agency's decision to withhold information, the burden of proof rests on the agency to sustain its decision, and the reviewing court is directed to "determine the matter de novo." 5 U.S.C. § 552(a)(4)(B).

At the same time, of course, it must be recognized that FOIA represents a carefully considered balance between the right of the public to know what their government is up to and the often compelling interest that the government maintains in keeping certain information private, whether to protect particular individuals or the national interest as a whole. *See John Doe Agency v. John Doe Corp.*, 493 U.S. 146, 152-53 (1989) (“The Act’s broad provisions favoring disclosure, coupled with the specific exemptions, reveal and present the ‘balance’ Congress has struck.”) As such, the exemptions must be given “meaningful reach and application.” *Id.* at 152. In a FOIA case, the agency generally meets its burden by providing affidavits describing the material withheld and the reasons that it fits within one or more of the exemptions. And, at least in the national security context, the reviewing court must give “substantial weight” to such affidavits. *King v. Dep’t of Justice*, 830 F.2d 210, 217 (D.C. Cir. 1987). In such cases, summary judgment may be granted based on an agency’s affidavits if they contain “reasonable specificity of detail rather than merely conclusory statements, and if they are not called into question by contradictory evidence in the record or by evidence of agency bad faith.” *Halperin v. CIA*, 629 F.2d 144, 148 (D.C. Cir. 1980).

## **II. Withholdings under Exemption 1**

Exemption 1 is FOIA’s national security exemption. *See Bonner v. Dep’t of State*, 928 F.2d 1148, 1150 (D.C. Cir. 1991). It allows an agency to withhold materials “(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order.” 5 U.S.C. § 5521(b)(1). While an agency’s declarations setting forth the reasons that information falls within this exemption are entitled to substantial weight, they must

nevertheless afford the requester an ample opportunity to contest, and the Court to review, the soundness of the withholding. *Campbell v. Dep't of Justice*, 164 F.3d 20, 30 (D.C. Cir. 1998) (observing that “deference is not equivalent to acquiescence”); *Goldberg v. Dep't of State*, 818 F.2d 71, 76-77 (D.C. Cir. 1987) (noting that Exemption 1 does not relieve the courts of their “independent responsibility” to review the agency’s decision).

Therefore, to justify summary judgment, an agency affidavit invoking Exemption 1 must provide “detailed and specific” information demonstrating both why the material has been kept secret and why such secrecy is allowed by the terms of an existing executive order. *Campbell*, 164 F.3d at 30; *King*, 830 F.2d at 217. If the declarations provide the requisite specificity, however, and are neither contradicted by other record evidence nor contaminated by indications of bad faith, the reviewing court should not ordinarily second-guess the agency’s judgment. Instead, the court must recognize that the executive branch departments responsible for national security and national defense have unique insights and special expertise concerning the kind of disclosures that may be harmful. *See Kirkorian v. Dep't of State*, 984 F.2d 461, 464 (D.C. Cir. 1993); *Salisbury v. United States*, 690 F.2d 966, 970 (D.C. Cir. 1982); *Military Audit Project v. Casey*, 656 F.2d 724, 738 (D.C. Cir. 1981). In other words, while the Court is ultimately to make its own decision, that decision must take seriously the government’s predictions about the security implications of releasing particular information to the public, at least where those predictions are sufficiently detailed and do not bear any indicia of unreliability.

The executive order in effect in this case is Executive Order 12,958. OIPR concluded that two documents responsive to plaintiffs’ FOIA request should be classified pursuant to this Order. The declaration of James Baker, OIPR’s Counsel for Intelligence Policy, explains the reasoning behind this decision. The two withheld documents are: (1) the classified answers

provided to HPSCI in response to the 50 questions posed by the Judiciary Committee, and (2) certain pages from the *Attorney General's Reports to Congress on FISA*, upon which DOJ relied in preparing those answers. (Baker Decl. ¶ 15.) Section 1.5(c) of the Executive Order lists “intelligence activities (including special activities)” and “intelligence sources or methods” among the kinds information that should be considered for classification. In turn, section 1.2 requires classification of such information where a determination is made that unauthorized disclosure of the information “reasonably could be expected to result in damage to national the security.”<sup>10/</sup> In his declaration, Baker explains that he carefully examined the two documents in question and concluded that their disclosure would have such an effect.

The contested documents “describe the frequency or manner of use of specific techniques authorized under FISA for use against clandestine intelligence and international terrorist activities.” (*Id.* at ¶ 16.) According to Baker, revealing this information would enable the potential targets of such surveillance “to conduct their intelligence or terrorist activities . . . more securely.” (*Id.* at ¶ 17.) Specifically, he continued, disclosing the number of times that DOJ has used its new “roving” surveillance authority could provide “critical information” about whether taking evasive action, such as changing telephones or e-mail accounts, would provide a safe harbor from FBI counterintelligence and counter-terrorism efforts. (*Id.*) Disclosing the number of U.S. persons who were the subject of FISA orders generally, or pen register/trap and trace devices more particularly, could provide an indication about whether and to what extent terrorist and foreign intelligence operations would be safer if they were to recruit such persons as their agents. (*Id.*) Finally, disclosing the number of FISA applications made for the production of

---

<sup>10/</sup> In this context “national security means the national defense or foreign relations of the United States.” Exec. Order No. 12,958, § 1.1(a).

tangible things could enable adversaries to discern whether and to what extent business records and other items in the possession of third parties offered a safe harbor from the FBI. (*Id.*)

While the FBI withheld a broader class of information under Exemption 1, plaintiffs contest the Bureau's withholdings "only insofar as the records indicate that total number of times the FBI has used particular surveillance and investigatory authorities during a specified time period." (Mem. in Support of Pls.' Mot. for Summ. J. at 24.) Plaintiffs thus do not take issue with the refusal to turn over other responsive material, which contains more detailed information linked to particular field offices or particular FISA investigations. As such, their challenge implicates virtually the same information contained in the documents withheld by OIPR. In particular, the contested materials are: (1) a report listing the total number of pen registers issued to FBI agents since October 26, 2001; (2) a report listing the number of requests for business records under FISA during the same period; (3) handwritten information about the total number of National Security Letters (administrative subpoenas used by the FBI to obtain various kinds of records) authorized during specific time periods; and (4) a document indicating the number of times each investigatory tool authorized by the Patriot Act has been used by the FBI. (Def.'s Mot. for Summ. J. on Behalf of the FBI, Ex. 4 [Kiefer Narrative].)

The FBI's justifications for relying on Exemption 1 echo those set forth by OIPR, although they are less specific. Indeed, for each the documents described above, the Bureau's records management attorney offers exactly the same defense:

It is my determination that the release of this information could reasonably be expected to cause serious damage to the national security, as it would: (1) allow hostile entities to discover what activities or methods the FBI is currently utilizing in its intelligence or counterintelligence gathering operations; (2) reveal the nature, objective, and requirements, of a specific FBI counterintelligence activity or method; and (3) disclose the intelligence-gathering capabilities of the activity or method. The release of this information

could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities within the specific areas and during a particular time frame. This would provide hostile agents with an evaluation of hostile intelligence plans and programs that have or have not been compromised and allow them to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as to make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense.

(Kiefer Narrative at 6, 8, 10, 64.)

This boilerplate lacks the detail and specificity of the Baker Declaration submitted on behalf of OIPR. The analysis here has in no way been tailored to the particular surveillance tools about which plaintiffs seek information, and does not address the specific harm likely to flow from the release merely of aggregate statistical information about those tools. In this respect, the FBI largely recites conclusions, rather than explaining the basis for those conclusions. *Cf. Goldberg*, 818 F.2d at 78 (“Conclusory and generalized allegations of exemptions are not acceptable.”) (internal quotation omitted). Nevertheless, plaintiffs concede (and the Court agrees) that DOJ's defense of its invocation of Exemption 1 – whether asserted by OIPR or by the FBI – must stand or fall as one. (Mem. in Supp. of Pls.' Mot. for Summ. J. at 24-25.) Indeed, the materials sought to be withheld are essentially the same in both cases, and it would make little sense to dictate that identical information held by different components of the same department should be simultaneously revealed and concealed merely because one component has written a more persuasive declaration than the other.

Therefore, the Court's task is to determine whether the combined force of the affidavits submitted by OPIR and the FBI justifies the use of Exemption 1 to withhold the aggregate statistical information that each possesses. As already noted, the governing standard in this context is not especially onerous: the agency must demonstrate “a logical connection between

the information and the claimed exemption, and are not controverted by either contrary evidence in the record nor by evidence of agency bad faith.” *Abbots v. Nuclear Regulatory Comm’n*, 766 F.2d 604, 606 (D.C. Cir. 1985) (internal quotations omitted). “The test is not whether the court personally agrees in full with the [agency’s] evaluation of the danger—rather, the issue is whether on the whole record the Agency’s judgment objectively survives the test of reasonableness, good faith, specificity, and plausibility in this field of foreign intelligence in which the [agency] is expert and given by Congress a special role.” *Gardels v. CIA*, 689 F.2d 1100, 1105 (D.C. Cir. 1982).<sup>11/</sup> Having carefully reviewed the declarations submitted by DOJ, the Court concludes that they satisfy these requirements. While plaintiffs’ arguments in favor of disclosure are not without force, they are ultimately insufficient to overcome the agency’s expert judgment that withholding the disputed information is authorized by the Executive Order because it is reasonably connected to the protection of national security.

Plaintiffs’ central claim is that the disclosure of the information they seek cannot plausibly be distinguished from the disclosure of similar information that is already required by FISA itself. As noted above, section 107 of FISA requires the Attorney General to issue an annual report to the Administrative Office of the United States Courts setting forth the “total number of applications made for orders and extension of orders approving electronic surveillance,” as well as the total number of such applications “either granted, modified, or denied.” 50 U.S.C. § 1807. According to plaintiffs, this fact undermines the Baker

---

<sup>11/</sup> It should be noted that this “special deference” to the agency’s affidavits is unique to Exemption 1. See *Alyeska Pipeline Serv. Co. v. EPA*, 856 F.2d 309, 315 (D.C. Cir. 1988); *Ctr for Nat’l Security Studies v. Dep’t of Justice*, 215 F. Supp. 2d 94, 103 (D.D.C. 2002) (contrasting Exemption 1 cases with cases under other FOIA exemptions, where the government’s declarations are entitled to less deference).

Declaration's conclusion that withholding aggregate data regarding FISA surveillance and search provisions is necessary to protect national security. (Reply Mem. in Supp. of Pls.' Mot. for Summ. J. at 4-5.) If one category of statistics can be disclosed without harm, plaintiffs contend, every similar category of information must be made available to the public as well.

The first response to this argument is that Congress itself has already made the very distinction that plaintiffs now contend cannot be made. Under FISA, much of the statistical information that plaintiffs now seek, which relates to the use of particular surveillance and search tools, including pen registers and demands for production of business records, is subject to its own disclosure regime, which is separate and distinct from that imposed by section 107. As described in footnote 7, *supra*, such information must be provided only to the relevant congressional oversight committees, not to the public at large. *See* 50 U.S.C. §§ 1846, 1852. In other words, after specifically considering this issue, Congress ultimately chose not to insist upon the full public disclosure of the statistics that defendant has withheld, while simultaneously requiring such disclosure for other, arguably more general, statistical data. At the very least, this clear congressional choice undermines plaintiffs' claim that these two kinds of information cannot meaningfully be distinguished. In making its withholdings here, DOJ is therefore acting largely to maintain and defend a line that has previously been drawn by Congress.

Moreover, the existence of these separate disclosure channels suggests that section 107 was not intended to preclude the Attorney General from classifying statistical information not covered by that provision. Indeed, to use that requirement to compel the public disclosure of the information sought here would do violence not only to the limited language of section 107 itself, but also to the structure of FISA as a whole, which strikes a careful and considered

balance between the need for public scrutiny of government surveillance activities and the need for operational secrecy in carrying out such surveillance. Thus, whatever assistance section 107 on its own might have provided to plaintiffs' case is severely limited by Congress' corresponding decision *not* to provide for the broad dissemination of the very data at issue here. Because this congressional balance is not lightly to be disturbed, the mere fact that FISA provides for the public disclosure of certain aggregate statistical data cannot mean that different, but *arguably analogous*, information must thereby automatically be disclosed under FOIA. Instead, the question must turn (as it always does) on whether the government has provided a specific and persuasive explanation of why such disclosures would be at odds with national security.

This is not to say that because the information plaintiffs seek is not available to them under FISA, they are necessarily precluded from obtaining it through FOIA. Rather, the point is that nothing in FISA either entitles them, explicitly or implicitly, to such information, or casts doubt on the reasonableness of defendant's conclusion that these statistics must be kept classified in order to protect intelligence sources and methods. In this sense, plaintiffs' invocation of section 107 is misplaced, and must not be allowed to distract attention from the fact that they have done little to challenge the Baker Declaration's determination that the disclosure of the statistical information contained within the classified answers may reasonably be expected to compromise national security by frustrating the counterintelligence and counterterrorism purposes of FISA (as amended by the Patriot Act).

And on this crucial point, the Court is satisfied that defendant's affidavits are sufficient to carry its burden. There is no basis in the record to dispel the government's basic concerns about the damage that may be done by the release of the numerical information at issue here.

Indeed, records that indicate how DOJ has apportioned its counterespionage resources, that reveal the relative frequency with which particular surveillance tools have been deployed, and that show how often U.S. persons have been targeted may undoubtedly prove useful to those who are the actual or potential target of such surveillance, and may thereby undermine the efficiency and effectiveness of such surveillance. That the public has a significant and entirely legitimate desire for this information simply does not, in an Exemption 1 case, alter the analysis. Defendant has provided an entirely reasonable explanation as to how national security may be jeopardized by the release of the information that plaintiffs seek. Because this account is undermined neither by contrary record evidence nor by any indication of agency bad faith, the Court is obliged to uphold DOJ's withholding, notwithstanding plaintiffs' compelling argument that the disclosure of this information will help promote democratic values and government accountability.

Plaintiffs make one further argument that the disputed information was improperly classified, and thus not protected by Exemption 1. They contend that because the Patriot Act shifted FISA's focus away from counterintelligence to more routine law enforcement, defendant is now precluded from relying on section 1.5(c) of Executive Order 12,958, which allows classification only to protect *intelligence* activities, sources, and methods. While ingenious, this argument is ultimately unpersuasive. To be sure, the Patriot Act did make it easier for the government to obtain a FISA surveillance order for purposes of mounting a criminal prosecution. Under the previous version of FISA, before the government could obtain an order to conduct electronic surveillance or a physical search, it had to certify to the FISA court that "the purpose" of the surveillance or search was to obtain foreign intelligence information. The Patriot Act altered this standard, changing the operative language from "the purpose" to "a

significant purposes.” Patriot Act, § 218, *amending* 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B). Thus, plaintiffs correctly point out that the amended FISA allows DOJ to obtain a surveillance or search order where its primary purpose in making the request is to gather evidence to initiate a criminal prosecution against the targeted foreign agent. *See In re Sealed Case*, 310 F.3d at 732 (“There is simply no question . . . that Congress was keenly aware that this amendment relaxed a requirement that the government show that its primary purpose was other than criminal prosecution.”).<sup>12/</sup>

However, it is clear that even after the Patriot Act, the government may take no action under FISA unless a “significant purpose” of the surveillance or search is to obtain foreign intelligence information. As such, every order approved under FISA, and thus accounted for in the statistics that defendant has classified here, necessarily involves the gathering of intelligence information as a non-trivial part of its purpose. All such orders thus fall logically within the ambit of the relevant provision of the Executive Order, and therefore within the protection of Exemption 1. This is simply not true of the Title III surveillance warrants to which plaintiffs seek to draw an analogy. *See* 18 U.S.C. § 2519 (setting forth the government’s broad disclosure obligations with respect to surveillance conducted for law enforcement purposes under Title III, 18 U.S.C. § 2510 et seq.). While it may be that a *particular* Title III warrant was obtained (in

---

<sup>12/</sup> It should be noted, however, that even under the amended FISA, the government’s power to use the statute for general law enforcement purposes remains limited. In its first (and to date only) decision, the Foreign Intelligence Surveillance Court of Review rejected the argument that “the Patriot Act allows the government to have a primary objective of prosecuting an agent for a non-foreign intelligence crime.” *In re Sealed Case*, 310 F.3d at 736. Thus, while the Court read the amended version of § 1804(a)(7)(B) to allow the government to obtain a FISA order where its primary purpose was to obtain evidence to prosecute a “foreign intelligence crime” (so long as that is not its sole purpose), the Court flatly rebuffed the suggestion that FISA process may “be used as a device to investigate wholly unrelated ordinary crimes.” *Id.* at 735-36.

part) to obtain intelligence information, statistics listing only the *total* number of Title III warrants issued during a particular period would reveal little, if anything, about the nature of the government's intelligence-related operations. This is so because there is simply no necessary connection between such warrants and covert intelligence activity, and therefore no indication as to how many of a given set of Title III warrants may have had such a link. In the FISA context, by contrast, even aggregate data is revealing, because it is a mandatory condition of every surveillance order that the government's application directly implicate foreign intelligence. Because nothing in the Patriot Act alters this fact, its provisions cast no doubt whatsoever on the reasonableness of DOJ's decision to classify the information at issue here.

Accordingly, the Court concludes that defendant's explanation of why it has withheld aggregate statistical information revealing the number of times it used particular Patriot Act surveillance and search tools is sufficiently detailed and persuasive to satisfy the standards for protecting agency records pursuant to FOIA Exemption 1.

### **III. Withholdings under Exemption 5**

Exemption 5 allows an agency to withhold memoranda or letters that would be protected from discovery in routine civil litigation. *See* 5 U.S.C. § 552(b)(5). This provision has been interpreted to incorporate the deliberative process privilege, which shields from disclosure documents that reflect or reveal the deliberations in which an agency engaged before arriving at a decision on a particular policy question. *See Tax Analysts v. IRS*, 294 F.3d 71, 76 (D.C. Cir. 2002). The critical question in this context is whether "disclosure of the materials would expose an agency's decisionmaking process in such a way as to discourage candid discussion within the agency and thereby undermine the agency's ability to perform its

functions.” *Formaldehyde Instit. v. Dep’t of Health and Human Servs.*, 889 F.2d 1118, 1121-22 (D.C. Cir. 1989) (quoting *Dudman Communications Corp. v. Dep’t of the Air Force*, 815 F.2d 1565, 1568 (D.C. Cir. 1987)). To receive protection, therefore, the materials must be *both* predecisional and deliberative. See *Mapother v. Dep’t of Justice*, 3 F.3d 1533, 1537 (D.C. Cir. 1993).

Purely factual information is generally considered non-deliberative, and is therefore not typically covered by this exemption. See *Coastal States Gas Corp. v. Dep’t of Energy*, 617 F.2d 854, 857 (D.C. Cir. 1980). Such information must therefore be disclosed even when contained in an otherwise protected document, unless the factual material is “inextricably intertwined” with, or incapable of being segregated from, the exempt material. See *Army Times v. Dep’t of the Air Force*, 998 F.2d 1067, 1071 (D.C. Cir. 1993) (“Exemption 5 applies only to the deliberative portion of a document and not to any purely factual, non-exempt information the document contains. Non-exempt information must be disclosed if it is reasonably segregable from exempt portions of the record, and the agency bears the burden of showing that no such segregable information exists.”) (internal quotations omitted); *Brinton v. Dep’t of State*, 636 F.2d 600, 605-06 (D.C. Cir. 1980).

Here, while defendant has asserted that Exemption 5 applies to a number of documents, plaintiffs challenge these withholdings only insofar as DOJ has refused to release “segregable factual information,” *i.e.* aggregate statistical data contained within predecisional documents, but separate and distinct from the deliberative portions of those documents. (Mem. in Supp. of Pls.’ Mot. for Summ. J. at 26 n.18; Reply Mem. in Supp. of Pls.’ Mot. for Summ. J. at 10.) To evaluate this objection, the Court has had to look carefully at withholdings made by each DOJ component involved in this case. First, with respect to OIP, it is now clear that the material at

issue does not contain the sort of information that plaintiffs seek. The original declaration submitted by OIP asserted that intra-agency e-mails withheld under Exemption 5 addressed “which Department components should be tasked with working on particular questions, *what the answers might consist of*, and what language should be used in the response letter.” (Sec. Pustay Decl. ¶ 12 (emphasis added).) While this language is perhaps ambiguous, a subsequent OIP declaration clarifies that in fact none of the e-mails contain “statistical information regarding the use of the various provisions of the Patriot Act.” (Third Decl. of Melanie Pustay ¶ 4.) The Court accepts this representation, which effectively undermines plaintiffs’ sole objection to OIP’s assertion of Exemption 5.

The situation for OIPR and the FBI is more complicated because it was not clear from the original record whether any of the documents withheld by these components actually contain factual information of the sort sought by plaintiffs. First, OIPR’s declaration says only that certain e-mails discuss “what approach should be taken in responding to the [House Judiciary Committee’s] questions.” (Baker Decl. ¶ 24.) While plaintiffs believe that this language suggests the presence of statistics, this simply could not be determined from defendant’s papers. Similarly, one of the declarations submitted by the FBI indicates that one document (drafted by Charles Steele, the Bureau’s Deputy General Counsel) includes “a collection of statistics, thoughts, idea and proposals” generated in response to Congress’ request for information on the implementation of the Patriot Act. (Decl. of Charles Steele [Steele Decl.] ¶ 9.) However, another FBI declaration, describing the same document, makes no mention of statistics, reporting only that the Steele’s memorandum “is a collection of thoughts, discussions, ideas, proposals, and proposed recommendations. . .” (Kiefer Decl. ¶ 38.) In order to resolve these conundrums, the Court requested that DOJ provide these disputed OIPR and FBI

documents for *in camera* review. See 5 U.S.C. § 552(a)(4)(B).

Now that defendant has done so, it is clear that its withholdings are proper. Indeed, the documents reveal that plaintiffs' Exemption 5 attack "thrusts largely at lions of [its] own imagining." *Bd. of Educ. of Kiryas Joel Village Sch. Dist. v. Grumet*, 512 U.S. 687, 708 (1994). The Court has reviewed the OIPR e-mails (a total of 29 pages), and determined that they contain no factual or statistical information whatsoever. Instead, these documents consist of paradigmatic Exemption 5 material: intra-agency conversations concerning the best ways to respond to the Judiciary Committee's questions, including suggestions for stylistic changes in proposed language, exchanges about the meaning and scope of certain questions posed by Congress, and discussions of how to provide responsive answers in a way that would not compromise national security. Refusing to disclose this entirely deliberative information is entirely appropriate, and plaintiffs do not suggest otherwise. With respect to the FBI document, while it does contain a few notations that relate to the frequency with which particular Patriot Act provisions have been used, the Bureau has in fact classified this information, and withheld it pursuant to Exemption 1.<sup>13/</sup> The Court has already approved this withholding, which moots plaintiffs' Exemption 5 argument. As such, *in camera* review has demonstrated that there is simply no factual information that defendant has tried to withhold under Exemption 5, and thus no substance to plaintiffs' challenge under that provision.

---

<sup>13/</sup> Having examined this document, which consists of a collection of handwritten notes scribbled on a copy of the Patriot Act's table of contents, it is clear that this is in fact the same document that occupies pages 77 and 78 of FBI Exhibit 1. In the Kiefer Narrative, the Bureau justifies its withholding of the statistical information contained in these pages under Exemption 1, which is consistent with the FOIA annotations that appear on those portions of the document. (Keifer Narrative at 63-64.)

## CONCLUSION

For the reasons given above, the Court holds that DOJ properly invoked Exemption 1 to withhold aggregate statistical data concerning its use of specific provisions of the Patriot Act, and that plaintiffs' limited challenge based on Exemption 5 is, on the facts presented here, without merit. Defendant's motions for summary judgment will therefore be granted.

---

ELLEN SEGAL HUVELLE  
United States District Judge

DATE: May 19, 2003

